TOP SECRET

CSDIC/CMF/Y 38

THIRD DETAILED INTERROGATION REPORT

Copy No:- 13

ON L/Cpl COELER Gerd

I FOLDER
#122

Name	:	COELER Gerd.
Rank	:	L/Cpl.
Unit	:	7 INTERCEPT EVALUATION SEC.
FP No.	:	05018.
Captured	:	BREGANZE, about 1 May 45.
Secret No	:	M 45/584.
Interrogated	:	CSDIC, CMF, 30-31 May 45.

This report should be read in conjunction with CSDIC/CMF/Y 30 and 31. It contains infm concerning trg and syllabus of a cryptography course run at OKH IN 7/VI. The original German text is given, as written out by PW in reply to questions put to him, and a translation is attached. The text and translation have been altered as little as possible in order to show how PW's mind worked. PW's spelling of certain names - e.g. "SAIKO" for "SYKO" - has also been retained. PW gave the impression of being anxious to help. For history and other details see CSDIC/CMF/Y 30, paras 1 and 2.

(Interrogated by A.G.B. and J.P.)

+++++++++++++++++++++++

TRANSLATION

FILE COPY

DO NOT DESTROY OR MUTILATE

CRYPTOGRAPHY COURSE

(Held at OKH/In 7/VI, BERLIN,
from mid-Oct 41-beg Jan 42)

PART I - INTRODUCTION

Duration of Course: 10 weeks.

Selection of Candidates: This was done after they had been examined at the Sigs Interpreters Depot Bn., MEISSEN, as to their suitability. They were examined by the OC Course.

OC Course: Oberinspektor KUEHN of In 7/VI.

O i/c my Course: Sonderfuehrer (Z) MARQUARDT.

O i/c Course being held at the same time: Uffz NOWAK.

Language Instructor: Sdf (Z) KOEHLER. He was detailed to instruct both Courses.

Working Hours: 0815-1200 and 1400-1730 hrs daily, except Saturday afternoons and Sundays, which were free.

All interpreters belonging to the various language groups at MEISSEN attended the Course, irrespective of the particular Referat in which they would later be employed. All students knew enough English for cryptographic purposes.

5-5127 #
ENV

The syllabus provided for instruction in cryptography during the morning and two or three afternoons a week, while English military terms, English history and geography were taught during the remaining afternoons.

I. CRYPTOGRAPHY

By way of introduction, we were told about the history of cryptography and its development. After being given a general picture of the methods of enciphering (substitution and transposition), we were taught details of the various ways of enciphering, orthodox and unorthodox methods of deciphering (breaking).

1. Substitution Methods

We were first instructed in the various polyalphabetic ciphers (see Part II). Instruction was verbal and by blackboard. After this, and after the methods of solution had also been demonstrated on the blackboard, each student was given practice problems (based on clear English text) to solve for himself. The SYKO machine, syllabic codes and code books were also dealt with at this stage. Of these, the English W.O.C. was treated in greater detail; and, based on this, students were explained the general methods of breaking the recipher and (relative) reconstruction of a code-book.

2. Transposition Methods

All main types or forms of transposition cipher (rectangles, squares, complete and incomplete) were taught. Instruction in the various transposition cipher methods (see Part II) and methods of solution, together with practical test-problems, was given as in para 1 above. The RASTER were also dealt with at this stage.

3. Other Methods

As regards other forms of enciphering (such as combined methods and machine cipher) in use at the time, only a general picture of their construction was given, without any details concerning methods of solution.

II. ORAL INSTRUCTION

The following subjects were taught orally:-

1. English Military Terms and Abbreviations, including a study of the organisation of the English Armed Forces, the different arms of the Services, formations, units and badges of rank. Use was made of German and English handbooks. Practice tests were held to find out how much had been learnt.

2. History and Organisation of the British Empire

Lectures on this subject were sometimes given in English.

3. Geography of ENGLAND

Students were expected to show knowledge of the various counties, towns, rivers, etc., and their exact positions. The following is an example of the kind of test employed: Each student was given an outline map of ENGLAND, with numbers indicating the position of the towns. The student had to write down the names of the towns corresponding to the various numbers.

III. OTHER SUBJECTS TAUGHT

Considerable attention was paid to instruction in security, espionage and counter-espionage.

On completion of the course, students were sent to the various Referate or Aussenstellen for which they were considered most suitable, or were returned to their unit as unsuitable.

Note:

1. Attempts to train women cryptographers on courses did not usually meet with success. In spite of this, considerable use was made of women assistants during the later stages.
2. The oral part of the instruction was subject to ever-increasing restrictions during the later courses.

PART II - SYLLABUS OF COURSE

(The under-mentioned methods of enciphering, as taught on the Course, are grouped according to procedure and not according to the amount of time devoted to their study)

I. SUBSTITUTION METHODS

Characteristic: According to statistics there are, in the absence of recipher or other complications (such as variants, etc.), so-called "frequencies typical of polyalphabetic cipher", i.e. there are no high-frequency letters, and the cipher letters must be identified with their corresponding clear letter according to their percentage frequency. It follows that, the shorter the text to be enciphered, the greater the margin of error, and statistics cannot now be regarded as anything more than a limited aid to purely intuitive textual breaking-in (of ciphers).

A. A Clear Symbol (letter, figure, syllable, word, etc.) is replaced by a Cipher Symbol:-

1. Simple ~~Polyalphabetic Cipher~~ substitution with standard alphabet

a) Alphabetic simple polyalphabetic cipher:

Clear alphabet : ABCDE.....
Cipher alphabet : DEFGH.....

Example of enciphering:-

Clear text : BAD DAY.....
Cipher text : EDG GD......

b) ~~Reciprocal~~ simple ~~polyalphabetic~~ substitution cipher:- with reversed std alph.

Clear : ABCDE.....
Cipher : ZYXWV.....

(Method of enciphering as for (a) above)

c) Normal simple ~~polyalphabetic~~ substn cipher:- with mixed alph.

Clear : ABCDE.....
Cipher : GAZXI.....

(Enciphering as for (a) above)

2. Polyalphabetic Cipher with Variants

This can take several forms. When enciphering a clear letter by means of a cipher symbol it is only possible to do this with variants by taking the ten figure symbols in addition to the alphabet letters. In such cases the ten figures are either allotted as variants to the ten high frequency letters of the alphabet, or alternatively three variants are allotted to a few frequent letters and the remainder to the next frequently occurring ones. It follows then that the frequencies are altered and that peaks in frequency graphs cannot be found easily.

Clear :	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	. . . .
Cipher:	C		T		1			B	Z	A	9		7	M	D			G	X		
	Y				L				5				C	N	F			H	3		
					0														8		

Example of enciphering:

Clear : ATTACK
Cipher: CX3YTA

Figures are enciphered by using clear words, e.g. 7 = seven, etc. The other forms of polyalphabetic cipher with variants will be discussed later.

3. Polyalphabetic Cipher of regular pattern

The number of alphabets in polyalphabetic ciphers of regular pattern varies between 3 and 40.
The following is an example of a polyalphabetic cipher of 3 alphabets of regular pattern:-

Column 1		Column 2		Column 3		Column 4 = Col 1	
Clear	Cipher	Clear	Cipher	Clear	Cipher	Clear	Cipher
A	X	A	I	A	F	A	X
B	G	B	L	B	A	B	G
C	A	C	K	C	S	C	A
D	H	D	B	D	Z	D	H
.	.	.	.	.	.	.	.

Example of enciphering:-

Clear : BAD DAY....
Cipher: GIZ HI.....

Alphabetical polyalphabetic ciphers of regular pattern are, of course, also possible, but are not generally used. On the other hand, polyalphabetic ciphers with variants occur more frequently. The SYKO machine comes under this category. It is built on the principle of a 32 alphabets polyalphabetic cipher of regular pattern, except for the difference that the message can start anywhere within the first 10 columns (this is given by the indicator group). Each line can also start anywhere within the first 10 columns.

4. Polyalphabetic Cipher-hatted

This is similar to a polyalphabetic cipher of regular pattern, except that the sequence of alphabets is hatted, e.g.:-

Col 1. Col 2. Col 3. Col 4 | Col 5 = 2 Col 6 = 1

DECLASSIFIED
Authority EO 13526

Possible variations can be worked out as at 3 above.

B. A clear symbol is replaced by two cipher symbols:-

1. Polyalphabetic Cipher with variants (?)

In this instance the clear symbol is replaced by 2 letters or 2 figures so that if, for instance, figures (cipher) are taken, 100 cipher symbols are available, i.e. clear letters can be given from 3 to 5 variants.

Example:-

Clear :	A	B	C	D	E	.	.	.
Cipher :	03	09	13	..	..	..		
	74	11	24	..	..			
	82	17	35		..			
	91		48					
	97							

Almost all E.C.s (English Cipher) can also be said to have originated from the polyalphabetic cipher with variants in which however one clear symbol is replaced by 2 letters. In the case of this kind (type) of system known up to that time (1941/42) a card of 26 x 26 was used, containing clear syllables and/or words (676). In addition cards also contained letters (for spelling) and figures. All clear symbols were indicated (expressed) - as in a coordinates system - by means of two letters taken from two hatted alphabets.
Note: The TAUSCHTAFEL and the SLIDEX, which are of more recent date, are also based on this system.

2. The two-letter and/or two-figure syllable code

Generally arranged in the form of a book, it can be alphabetical as well as non-alphabetical. In addition to clear syllables, clear letters and figures can also be replaced by code symbols so that all clear words or text can be encoded. Two-letter codes are generally favoured, as a greater number of code bigrams (676) is available in such cases.

3. The two-letter and/or two-figure code-book ("WORD" code)

As for 2. above, except that instead of clear syllables, clear words were encoded by means of letters or figures.
Note: In practice clear words, syllables, letters and figures are all combined in one code book (2. and 3. above).

C. A clear symbol is replaced by three cipher symbols

This method is mostly used only in the form of three-figure codes (Lay-out as at B.3. above).

D. A clear symbol is replaced by four cipher symbols

This type of code appears in the form of four-figure codes. (Lay-out as at B.3. above). Breaking is made more difficult by use of recipher, such as for instance the subtractors or adders. In the case of the WOC it took the form of a practically unending, unperiodical figure-recipher.

E. A clear symbol is replaced by five cipher symbols

The only practical example quoted was the Russian five-figure code.

II. TRANSPOSITION METHODS

Main characteristic is that statistics always produce normal clear text frequency data.

A. ~~Anagramming~~:- Line transposition.

This is only used for short texts. It lacks security. Similar to "visiting card puzzles".

Example:- 2 5 1 7 8 4 6 3

Clear : F A B E R M A X
Cipher : B F X M A A E R

B. The transposition patterns (squares, rectangles, etc.)

1. The simple transposition pattern

a) The complete simple transposition pattern, is the easiest form of this type of cipher. The width of the pattern varies. The most common ones vary from 7 to approx 25. The text is written out from left to right and read out, in columns, from top to bottom, according to a figure key or a key-word written above the pattern.

Example:-

Clear :

3	1	4	6	7	5	2
R	E	F	Y	O	U	R
M	E	S	S	A	G	E
F	R	O	M	J	A	N

Cipher : EERRE NRMFF SOUGA YSMOA J

b) The incomplete simple transposition pattern, as at a) above, except that the last line in rectangle or square is not complete and that therefore the depth of the figure in certain columns differs by 1. This can render breaking considerably more difficult.

2. The "serpentine" transposition cipher

The clear text is written down as in 1.a) above. The only difference lies in the method of reading enciphered text out. This takes place as follows: Column marked 1 is read out from top to bottom,
" " 2 " " " " bottom to top,
" " 3 " " " " top to bottom, etc.

Kamm = comb!

3. The "cam-cube" or transposition pattern with incomplete rectangle

Example:-

Clear:

2	4	3	6	7	5	1
R			E			F
Y		O	U	R		M

Cipher: FMFRY EROSM SOEEU ARG

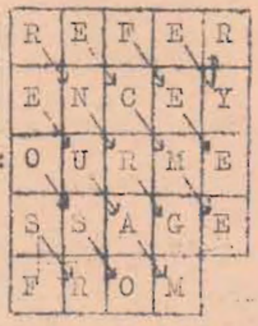
DECLASSIFIED
Authority EO 13526

This type of cipher can also take the form of "serpentine" transposition cipher.

4. The Diagonal Transposition cipher

The clear text is written down as for 1.a) above. Reading out is done with or without a key, diagonally, as agreed beforehand between the addressor and addressee. Many variations can be used, for instance, also in the form of a "serpentine" pattern. Example of one method of reading out a message:-

Clear:



R	E	F	E	R
E	N	C	E	Y
O	U	R	M	E
S	S	A	G	E
F	R	O	M	

Cipher: FSROS OEUAM RNRGE
CMEFE EEYR

5. The Double Transposition cipher

Procedure at first is as in 1.a) above. The resulting cipher text is then re-written in the rectangle (Comment: PW stated "in another rectangle"; this is however thought to be an error, see example) and hatted once more.

Clear text:

3	1	4	6	7	5	2
R	E	F	Y	O	U	R
M	E	S	S	A	G	E
F	R	O	M	J	A	N

Reciphered:

3	1	4	6	7	5	2
E	E	R	R	E	N	R
M	F	F	S	O	U	G
A	Y	S	M	O	A	J

The final cipher text is then: EFYRG JEMAR FSNUA RSMEO O....
The second pattern (rectangle) can, of course, have any other shape, width and key.

6. The "RASTER"

a) The simple "RASTER"

The principle is the same as in the "CAM CUBE" (transposition pattern with incomplete rectangle) when hatting or anagramming takes place according to a key. When no hatting or anagramming takes place, the blank spaces in the pattern are filled in (with clear letters) with the result that the clear text appears in a practically regular sequence, but with numerous breaks.

b) The "REVOLVING RASTER"

Contd

This is a particularly complicated form of cipher derived from the "CAM-CUBE" and developed from the simple hatted "RASTER" described at a) above. Entering or writing in of clear text is not done continually from left to right, but the use of the denting (changing pattern) of the stencil is changed four times; this is done by revolving the stencil periodically through 90°.

III. COMBINED METHODS

It is, of course, also possible to combine the various basic systems in order to get a combined cipher, or a cipher with recipher. Examples: The reciphered 4-figure code mentioned above, an anagrammed polyablphabetic cipher, a polyalphabetically reciphered transposition pattern, a letter-TAUSCHTAFEL, etc.

IV. MACHINE CIPHER

This cipher built up on the principle of a practically unending polyalphabetical cipher of regular pattern was mentioned on the course for academic interest only.

for (W.S. VALENTINE),
Lt-Col,
Comd, CSDIC, CMF.

C.S.D.I.C.,
C.M.F.
30 Jun 45.

EZ-Kursus

(bei OKH/In 7/VI, Berlin, Mitte Okt 41 bis Anf. Jan 42)

Dauer: 10 Wochen.

Auswahl: nach Eignungspruefung bei der Nachr. Dolm. Ers. Abt. in Meissen durch:

Gesamtleiter: Oberinspektor Kuehn von der In 7/VI.

Leiter meines Kursus': Sonderfuehrer (Z) Marquardt.

Leiter des Parallelkursus': Uffz Nowak.

Als Sprachlehrer beigeordnet (fuer beide Kurse): Sdf (Z) Koehler.

Arbeitszeit: 0815-1200, 1400-1730 (Samstag Nachmittag u. Sonntag frei).

Im Kursus waren saemtliche von den verschiedenen Meissner Sprachgruppen kommenden Dolmetscher vereint, ohne Ruecksicht auf ihre spaetere Verwendung in einem bestimmten Referat. Alle Teilnehmer konnten ein zumindestens fuer die EZ-Arbeit ausreichendes Englisch.

Der Kursuslehrplan war so aufgeteilt, dass vormittags und an 2-3 Nachmittagen Entzifferung gelehrt wurde, waehrend an den uebrigen Nachmittagen militaerisches Englisch, englische Geschichte und Geographie unterrichtet wurde.

I. Zur Entzifferung:

Als Einleitung wurde uns zunaechst die geschichtliche Entwicklung der Chryptographie aufgezeigt. Nach einem generellen Ueberblick ueber die Moeglichkeiten der Verschluesslung (Ersatzverfahren, Versatzverfahren) begann die eigentliche Einweisung in die einzelnen Verschluesslungsarten, ihre befugte und unbefugte Entschluesslung (= Entzifferung).

1. Ersatzverfahren:

Als Erstes wurden uns die verschiedenen Caesarenformen (siehe Gliederung!) erklaert. Die Erklaerung geschah muendlich and schriftlich an einer Wandtafel. Nachdem auch die Loesungsmethoden an der Tafel demonstriert worden waren, wurden an die einzelnen Kursusteilnehmer Uebungsbeispiele (mit zugrundeliegendem englischen Text) zum selbstaendigen Loesungsversuch verteilt. Auch die Saicomaschine, sowie Silben- und Woertercode wurden hierbei behandelt. Ausfuehrlicher wurde von letzteren der englische WOC behandelt, und an Hand dessen ganz allgemein die Moeglichkeiten der Entwurmung und relativen Erstellung eines Codes erklaert.

2. Versatzverfahren

Als deren Hauptformen wurden die Wuerfel besprochen. Erklaerung der verschiedenen Wuerfelarten (siehe Gliederung!), sowie ihrer Loesungsmoeglichkeiten mit anschliessenden praktischen Uebungsbeispielen wie bei 1. Hierbei wurden auch die Raster behandelt.

3. Sonstige Verfahren

Ueber die uebrigen zur Zeit auftretenden Verschluesslungsformen (wie kombinierte Verfahren und Maschinenverfahren) wurde nur ein allgemeiner Ueberblick ueber ihren Aufbau gegeben ohne naeher auf die Loesungsmoeglichkeiten einzugehen.